DRN-4369241

The complaint

Mr D complains that Citibank UK Limited (Citi) wouldn't refund money he lost in an investment scam.

What happened

What Mr D says:

Mr D had an account with Citi. His father was in a nursing home and he needed money to help pay for his medical fees. In May 2022, he was contacted via social media by a trader who claimed he was making money by trading with a bitcoin company. Mr D did some research and found the trader had many followers on social media. And he saw the bitcoin company was regulated in the UK and US. The trader asked him to open an account with a crypto exchange (which I will call 'A'). Mr D transferred money into his Citi account and then made payments to his crypto wallet:

Date	Payment / Beneficiary	Amount	Balance
8 September 2022			0.76 credit
12 September 2022	Faster Payment In/Mr D's Citi account	(£1,598)	£1,598 credit
14 September 2022	Faster Payment – crypto wallet A	£1,590	£8.81 credit
20 September 2022	Faster Payment In/Mr D's Citi account	(£4,000)	£4,008.81 credit
20 September 2022	Faster Payment – crypto wallet A	£4,000	£8.81 credit
Total		**£5,598**	

Mr D made some other payments from another bank account – which is the subject of a separate complaint to this service.

The trader coached Mr D to make payments from his crypto wallet to the bitcoin company. He was shown the website of the bitcoin company and it showed he was making profits. The trader asked him to pay more money such as a success fees, purchase of an access 'key', and insurance. Mr D then asked for profits to be returned, but none arrived.

Mr D realised he'd been the victim of a scam. The trader and the bitcoin company were fake. Mr D reported the scam to the police and Action Fraud. He thought he was dealing with a professional but was wrong. He says his mental health has suffered – and he has sleepless nights.

Mr D says Citi should've done more to protect him. He'd had an account with Citi for many years, and his account had been dormant for a long time before the scam. So – Citi

should've realised the payments were large and unusual.

What Citi says:

Citi said they'd made the payments in accordance with Mr D's instructions and in line with the Payment Service Regulations. Mr D had used the one-time password he'd been sent. The payments were sent to Mr D's own account in his name. They sent regular warnings to customers about fraud, and they warned clients they shouldn't ever act on a call out of the blue. Citi declined to refund any money.

Our investigation so far:

Mr D brought his complaint to us. Our investigator said the first payment was too small to have expected Citi to question it. But the second payment (for £4,000) should've been held by Citi and Mr D contacted about it. He said that because Mr D's account had been dormant for a year, the payment was out of character. If Citi had intervened, they'd have been able to question Mr D, found out he had been contacted via social media and the payment was typical of many similar scams, and so it was likely the scam would've been highlighted to Mr D and the payment prevented.

He said Mr D acted reasonably as he'd done research on the investment company, and the scammer had a large following on social media. Mr D had considered the website to be professional.

Our investigator said Citi should refund £4,000 plus interest of 8% per annum simple.

Citi didn't agree and asked that an ombudsman look at the complaint. They said the payments were to Mr D's own account (his crypto wallet), and he should approach A for reimbursement. They also evidenced a paper from UK Finance which said 'me to me' payments were not the liability of the sending bank.

What I've decided – and why

I've considered all the available evidence and arguments to decide what's fair and reasonable in the circumstances of this complaint.

I'm sorry to hear that Mr D has lost money in a cruel scam. It's not in question that he authorised and consented to the payments in this case. So although Mr D didn't intend for the money to go to a scammer, he is presumed to be liable for the loss in the first instance.

So, in broad terms, the starting position at law is that a bank is expected to process payments and withdrawals that a customer authorises it to make, in accordance with the Payment Services Regulations and the terms and conditions of the customer's account. And I have taken that into account when deciding what is fair and reasonable in this case.

But that is not the end of the story. Taking into account the law, regulators rules and guidance, relevant codes of practice and what I consider to have been good industry practice at the time, I consider Citi should fairly and reasonably:

- Have been monitoring accounts and any payments made or received to counter various risks, including anti-money laundering, countering the financing of terrorism, and preventing fraud and scams.
- Have had systems in place to look out for unusual transactions or other signs that might indicate that its customers were at risk of fraud (among other things). This is

particularly so given the increase in sophisticated fraud and scams in recent years, which banks are generally more familiar with than the average customer.

- In some circumstances, irrespective of the payment channel used, have taken additional steps, or make additional checks, before processing a payment, or in some cases declined to make a payment altogether, to help protect customers from the possibility of financial harm from fraud.

The CRM Code doesn't apply in this case because Citi hasn't signed up to it. But, taking into account the law, regulatory rules and guidance, relevant codes of practice and good industry practice, there are circumstances where it might be appropriate for Citi to take additional steps or make additional checks before processing a payment in order to help protect its customers from the possibility of financial harm from fraud.

If the payments were of a sufficient size and were out of character with how Mr D normally used his account – then we would expect Citi to have intervened and spoken to him about them. I looked at Mr D's account, and it's fair to say that the payments were unusual compared to the way in which he used his account – it was dormant for at least 12 months before the payments were made in September 2022.

First payment - £1,590 – 14 September 2022:

I don't consider Citi can be held liable for this payment. I say that as here's a balance to be struck: Citi has obligations to be alert to fraud and scams and to act in their customers' best interests, but they can't be involved in every transaction as this would cause unnecessary disruption to legitimate payments. In this case, the payment was for a relatively low amount, and therefore I think Citi acted reasonably in processing the first payment.

Second Payment - £4,000 – 20 September 2022:

I consider it's reasonable that Citi should've held this payment and contacted Mr D about it. I say that because:

- His account had been dormant for 12 months up to September 2022, with a balance of £1,606 credit. There was no account activity at all until Mr D made a payment for £1,600 on 7 September 2022 (not related to this complaint), reducing the balance to £6.76 credit.
- Then, there were two credits into the account just before the payments were made, one for £1,598.05, and one for £4,000 on 20 September 2022.
- The payment of £4,000 was made on the same day that the credit for £4,000 was received.
- The balance on the account was drained – to £8.81 credit after the second payment.
- The two payments were in relatively quick succession – within six days of each other – and were made after the account had been dormant for 12 months.
- The payment was going to a payment service provider which was known to provide crypto wallets to send money to bitcoin companies.

I'm also not persuaded that the fact the payments were going to Mr D's own account and so appeared to be going somewhere safe and within his control should have satisfied Citi that he wasn't at risk of harm. This is because by January 2019, firms like Citi had, or ought to have had, a good enough understanding of how these scams work – including that a customer often moves money to an account in their own name before moving it on again to the scammer - to have been able to identify the risk of harm from fraud.

So, on balance I'm satisfied there was enough going on here to say Citi should've intervened and contacted Mr D about the second payment.

If they had, I'm persuaded that enough warnings could've been given to Mr D for him to question the payment and not make it. Citi could've reasonably asked:

- Why are you making the payment?
- Who to?
- For what purpose?
- Where did the money come from that you're investing?
- How did you hear about the investment?
- How were you contacted?
- What do you know about bitcoin investing?
- Have you made bitcoin investments before?
- How were you given the bank account details where the money was to be paid to?

They'd have found out that Mr D knew nothing of bitcoin investments; that he was investing for the first time; that he had been contacted 'out of the blue' via social media; and the 'trader' had asked him to open the crypto wallet and had guided him to send money from there to the bitcoin company. And Citi could've given him sufficient warnings about what he was doing – and it was then unlikely he would've made the payment.

I've considered what Citi have said about the paper from UK Finance. I noted this was a consultation paper from the trade body and was dated September 2021. It's not policy. And here – our role is an impartial and informal dispute resolution service, reaching fair and reasonable decisions. And we take into account all relevant regulations and guidance in doing that. And we're satisfied that firms should still be detecting unusual transactions to cryptocurrency platforms (even in a customer's own name) – particularly due to the prevalence of these scams in recent years and after the publications from the regulatory, industry bodies and Action Fraud.

Citi have also said this decision goes against other decisions by this service. But – here I would say that each complaint is considered in the context of its own circumstances.

Contributory Negligence:

I considered whether Mr D could've done more to protect himself and whether he should therefore reasonably be responsible for some of his losses. But here, I'm persuaded he had done enough research. He looked up the bitcoin company online and found it was apparently registered in the UK and US; the 'trader' had a good following online; the website looked genuine and professional; and he was coached all along by the trader (who he had come to trust). So – I consider Mr D had done enough here.

Recovery:

We expect firms to quickly attempt to recover funds from recipient banks when a scam takes place. I looked at whether Citi took the necessary steps in contacting the bank that received the funds – in an effort to recover the lost money. I couldn't see that they'd contacted the provider of Mr D's crypto wallet – but I'm persuaded that had they done so, no funds would've remained – as he'd moved them into the bitcoin trading platform.

Putting things right

Citi should refund the second payment of £4,000, plus 8% per annum simple interest from

the date of payment to the date of settlement.

My final decision

I uphold this complaint. Citibank UK Limited must:

- Refund £4,000, plus 8% per annum simple interest from the date of payment to the date of settlement.

Under the rules of the Financial Ombudsman Service, I'm required to ask Mr D to accept or reject my decision before 16 November 2023.

Martin Lord
Ombudsman